

UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case No. 1:21-mj-751  
INFORMATION ASSOCIATED WITH CALL NUMBER )  
404-863-7483 AND/OR IMEI: 310410349684800 , THAT IS )  
STORED AT PREMISES CONTROLLED BY APPLE, INC. )

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Ohio  
(identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B (incorporated by reference)

**YOU ARE COMMANDED** to execute this warrant on or before Nov. 4, 2021 (not to exceed 14 days)  
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Karen L. Litkovitz  
(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 11:16 AM, Oct 21, 2021

City and state: Cincinnati, Ohio

Karen L. Litkovitz  
United States Magistrate Judge



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with TELEPHONE NUMBER **404-863-7483** AND/OR IMEI: **310410349684800** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple Inc. (“Apple”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all instant messages associated with the account from August 1, 2021 to Present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used; and

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).


Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

**Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 865 those violations involving Steffen ROBERSON and occurring after August 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence relating to the sale, purchase, and possession of illegal drugs, to include any preparatory steps taken in furtherance of the sale and possession of drugs;
- (b) Evidence relating to the identity of co-conspirators and drug customers;
- (c) Evidence related to the source of illegal drugs;
- (d) Evidence of any communications with co-conspirators; evidence of any steps taken in furtherance of drug trafficking and evidence of any steps taken to conceal the possession of drugs;
- (e) Evidence related to location of drug trafficking and storage of illegal drugs;

- (f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (i) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.

Return		
Case No.: <u>21-MJ-751</u>	Date and time warrant executed: <u>10/22/21 @ 10:00 AM</u>	Copy of warrant and inventory left with: <u>RETAINED IN CASE FILE</u>
Inventory made in the presence of: <u>CPD INTEL &amp; PO JONCE TACKETT</u>		
Inventory of the property taken and name of any person(s) seized: <u>STORED CONTENT OF APPLE ICLOUD ACCOUNT, TO INCLUDE:</u> <u>DEVICE INFORMATION, SUBSCRIBER INFORMATION, HISTORICAL</u> <u>LOCATIONS, CALL RECORDS, FACETIME LOGS, TEXT</u> <u>MESSAGES, PHOTOS, VIDEOS, AND ANY OTHER STORED</u> <u>DATA</u>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <u>2/17/22</u>	 Executing officer's signature	
	<u>BRANDON COOK, TFO</u> Printed name and title	